Google Chrome s'essaie au chiffrement post-quantique

Google s'apprête à l'arrivée des ordinateurs quantiques, qui promettent de révolutionner certains aspects du monde IT, par exemple le secteur du chiffrement, avec la capacité à décrypter des données jusqu'alors inaccessibles aux ordinateurs actuels.

« Si de grands ordinateurs quantiques sont construits alors ils pourraient être en mesure de ***briser les primitives cryptographiques asymétriques*** *qui sont actuellement utilisées dans TLS, le protocole de sécurité se trouvant derrière le HTTPS »*, explique **Matt Braithwaite**, ingénieur chez Google.

« De tels ordinateurs quantiques seraient capable de déchiffrer rétrospectivement ***toute communication Internet qui a été enregistrée aujourd'hui****, alors que certaines informations doivent rester confidentielles pendant des décennies. Aussi, la possibilité d'un futur ordinateur quantique est quelque chose à laquelle nous devrions penser dès aujourd'hui. »*

De nouvelles techniques de protection en test

Créer des primitives cryptographiques capables de résister aux ordinateurs quantiques de demain est le domaine de la **« cryptographie post-quantique »**. Un procédé que Chrome va expérimenter pour l'échange de clés entre le poste de l'internaute et les serveurs de Google. Un test qui ne s'appliquera pour le moment qu'à une fraction des transactions opérées auprès des serveurs de la firme.

Ce procédé est appliqué par-dessus les techniques actuelles, afin de ne pas affaiblir la sécurité des transactions, s'il s'avérait trop aisé à casser avec les ordinateurs d'aujourd'hui… ou de demain.

À lire aussi :
Google Chrome remet le contenu HTML tiers à sa place
Chrome accélérera avec la version 52 et mettra le turbo avec la 53
IBM met l'ordinateur quantique à la portée de tous, en mode Cloud

Crédit photo : © Pavel Ignatov – Shutterstock